Technical Study for Recommendations IoT Standardization in Fire Alarm Control Panel Systems

Fikri Nizar Gustiyana [1,3]*, Rendy Munadi [1], Nyoman Karna [1], and I Ketut Agung Enriko [2,3]

[1] Departement of Electrical Engineering, Telkom University, Bandung, Indonesia
[2] Departement of Telecommunication and Electrical Engineering, Institut Teknologi Telkom Purwokerto, Purwokerto, Indonesia
[3] Research and Innovation Management, Telkom Corporate University, Bandung, Indonesia
Email: fikrinizargustiana7899@gmail.com (F.N.G.); rendymunadi@telkomuniversity.ac.id (R.M.); aditya@telkomuniversity.ac.id (N.K.); enriko@ittelkom-pwt.ac.id (IK.A.E.)
*Corresponding author

***Abstract*—Fire Alarm Control Panel (FACP) components work together to detect fires, with IoT integration improving network connectivity. Standardization in IoT implementation in FACP systems is key to ensuring interoperability, security, and adequate data availability. Standardization is necessary to meet regulatory requirements and norms related to security. Until now, there are no international standards, as well as national standards in Indonesia, or specific technical recommendations for the selection and configuration of IoT systems in FACP systems. This research aims to recommend IoT standardization for FACP based on the results of technical tests for implementing the IoT system on FACP in terms of IoT Devices, IoT Networks, IoT Platform protocol, and IoT Applications. Based on the test results, it explores the connectivity options of IoT gateways, emphasizing their ability to interface with FACP via third-party interfaces with a validation rate of 100%, installing dual power sources, and increasing battery capacity. Cable networks are prioritized with backup internet connections, with Ethernet favored for its lower latency. The study suggests using HTTP or MQTT protocols for IoT platforms, aligning with established standards. For the IoT Application, comprehensive fire alarm status information, including location and detector status, is recommended. Usability testing validates these suggestions with high scores (Validation: 100%, SEQ: 5.4 – 6, SUS: 82, NPS: 100%), ensuring effective implementation of FACP IoT applications.**

***Keywords*—Fire Alarm Control Panel (FACP), IoT, standardization, QoS, fire alarm**

I. Introduction

Rapid growth in technology Internet of Things (IoT) has changed paradigms in various sectors, including security. One important security aspect is the Smoke and Fire Detection System (Fire Alarm and Control Panel - FACP), which is responsible for detecting, controlling, and providing early warning of fires. In the era of digitalization, IoT integration in FACP systems is becoming increasingly relevant to improve efficiency, reliability, and responsibility in the face of potential fire risks. FACPs consist of different elements like smoke detectors, heat sensors, alarms, and control panels that operate collectively to promptly identify and alert individuals inside a building in case of a fire emergency [1, 2]. When an initiating device like a smoke detector or manual pull station transmits an alarm signal to the Fire Alarm Control Panel (FACP), it triggers a notification mechanism to warn occupants using audible and visual alarm systems [3, 4].

With connectivity through IoT, FACP can become an integral part of larger networks, providing real-time access to data, and enabling better security management. Standardization in IoT implementation in FACP systems is key to ensuring interoperability, security, and adequate data availability [5]. Standardization is necessary to meet regulatory requirements and norms related to security. Compliance with standards can help an organization or company fulfill legal responsibilities [6]. Standardization can also help ensure the security of information passed through built telecommunications devices [7]. Until now, there are no international standards [8–10] as well as national standards in Indonesia, or specific technical recommendations for the selection and configuration of IoT systems in FACP systems. Some FACP system manufacturers may already have IoT solutions on their products [11] but it is certainly limited to functions that can only be used on the product. This can be an obstacle in the digitization process in the field of fire safety due to limited innovation in developing an IoT system so a standardization is needed on IoT devices that are universal in the FACP system to support innovators in developing their products following the standard.

This study aims to fill this knowledge gap and produce proposed recommendations for IoT standardization for FACP by investigating various relevant technical aspects

Manuscript received January 30, 2024; revised February 28, 2024; accepted March 7, 2024; published July 22, 2024.

by conducting literature reviews, system design, system implementation, and technical tests. The results of this study are expected to provide technical guidance and standard recommendations in the selection and configuration of IoT systems in the universal FACP system. This will help various parties to integrate IoT technology more effectively and ensure optimal safety and performance in the face of fire hazards. With clear standards in place, various security devices and IoT-enabled FACP systems can operate seamlessly together.

This paper is structured as follows: Firstly, a thorough literature study is conducted, sourcing information from various sources such as books, journals, and papers to inform the research. Following this, system planning and implementation take place, where the designed system is applied to the FACP system, accounting for problem constraints. Subsequently, data testing and analysis are performed to evaluate the system's performance against predetermined parameters. Finally, conclusions are drawn, and a thesis proposal report is prepared, featuring discussions, analysis of the system's design, and recommendations for further research.

II. Literature Review

A. Previous Research

The authors of [12] proposes a The integration of IoT devices, encompassing fire alarm components such as smoke and temperature detectors, alongside Arduino and supplementary equipment, constitutes a "Smart Fire Alarm System Using IoT" implemented in smart buildings. The objective of this research is to establish a mechanism wherein in the event of a fire, sensors transmit a notification to building security personnel, providing details regarding the location and time of the incident. IoT architecture in this study can be seen in Fig. 1.

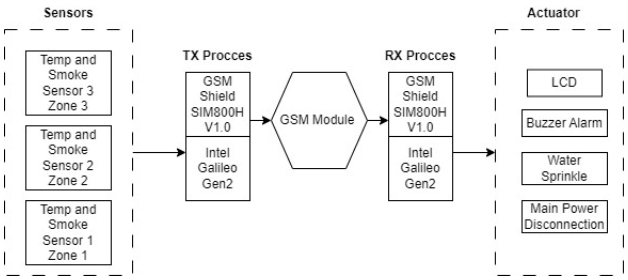

Fig. 1. Smart fire alarm system using IoT architecture.

According to the architecture, the installation of sensor groups is divided into three zones. The selected sensor is then connected to an Intel Galileo Gen2 analog pin board. There is a threshold value for each sensor, therefore the Galileo board checks the pins continuously so that if it receives a signal coming from one of the sensors, it will immediately compare the value of that signal with the pre-selected threshold value. Data is sent using the GSM network on the receiver side, and on the receiver side, there are several devices in the form of water sprinkles, LCDs, Buzzers, and Main Power Disconnection. This research has the advantage of making an end-to-end system based on IoT architecture. However, this study has not discussed IoT-related standardization in FACP.

The authors of [13] discusses IoT implementation on the device's Fire Suppression in more detail on the device Hydrant. This research aims to integrate Diesel Hydrant and Electric Hydrant devices in IoT systems using IoT Gateway devices with the following system architecture.

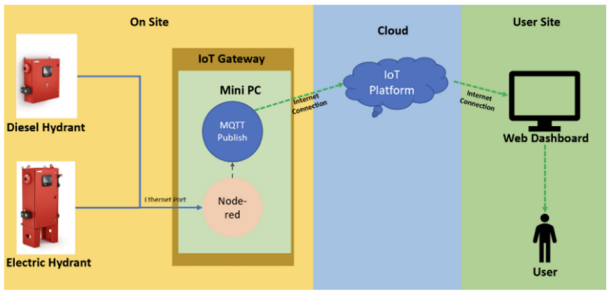

Fig. 2. Fire suppression monitoring architecture.

According to research [13], IoT Gateway is connected to Diesel and Electric Hydrant Panels using Modbus TCP, in addition to the protocol used in sending data to the IoT Platform using the MQTT protocol. The results of this study show that the implementation of IoT gateway can be implemented well with Quality of Service and Very good data delivery.

Then, the authors of [14] explained that the NFPA 72 standard has already issued permission to do so Remote Access Monitoring Along with the development of technology in the current era. In the article, it is explained that monitoring via the Internet does not have its title in the 2007 edition of NFPA 72; however, this is generally discussed in Section 8.6.4, "Other Transmission Technologies." As stated in the NFPA 72 document. The article also explains the proposal for centralized monitoring so that each connected FACP panel can send data to the monitoring center for 24 hours with a duration of every 300 seconds, it can help monitor Real-time which can minimize the possibility of a fire occurring.

However, the article does not discuss the standardization of systems that can be used on FACP devices to perform Remote Access Monitoring. So to complement this, this research can discuss the standardization of possible devices for Remote Access Monitoring centrally.

B. Fire Alarm Control Panel (FACP)

Fire Alarm Control Panel (FACP) serves as the central governing component within a fire alarm system. It receives signals from initiating devices such as smoke detectors, heat detectors, manual pull stations, and fire detectors. Subsequently, the panel activates various functionalities to notify occupants and emergency responders. Fire alarm panels are typically categorized into two primary types: conventional panels and addressable panels. Conventional panels operate by being installed within designated zones and detecting alterations in electric current within those zones. Conversely, addressable panels employ more advanced and programmable technologies with enhanced specificity.

FACPs are commonly positioned near building entrances or in enclosed areas, equipped with additional signaling devices to ensure audible notification for the designated administrator [1, 2]. The FACP block diagram can be seen in Fig. 3.

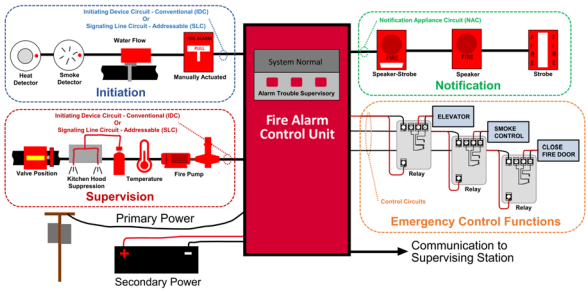

Fig. 3. Fire suppression monitoring architecture.

C. Internet of Things (IoT)

The Internet of Things (IoT) is a concept where various devices can connect and communicate with each other over the Internet to enable automated data collection and exchange [15]. Internet of Things (IoT) is a network of physical objects or devices, such as smart devices, wearables, vehicles, and buildings, equipped with sensors, device software, and the possibility of network connectivity to collect and exchange data [16]. The aim of the Internet of Things (IoT) is to establish a network of interconnected devices capable of automating tasks, enhancing efficiency, and introducing novel services and interactions. IoT architecture refers to the framework through which IoT devices establish connections, communicate, and collaborate to accomplish predefined objectives. The IoT architecture consists of four main layers which are Device, Network, Platform, and Application can be seen in Fig. 4 [13].

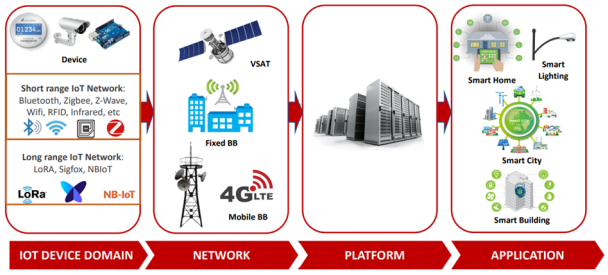

Fig. 4. Internet of Things architecture.

III. Research Methods

A. System Design

This study examines the IoT architecture section to create a system that can monitor the FACP System based on IoT architecture rules and FACP standardization that is already available (Standardization includes hardware specifications and other information). The IoT system that is designed is then implemented on the FACP that is already available in the Simulation lab for the research following the standards collected and then carried out testing to recommend new standards specifically for IoT systems on the FACP. An illustration of the research position can be seen in Fig. 5.

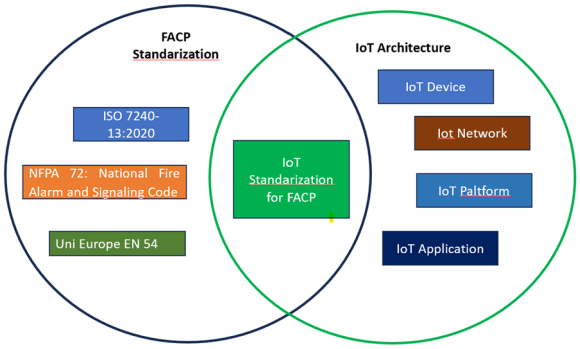

Fig. 5. Research positioning.

The IoT Architecture for the Fire Alarm Control Panel (FACP) is formulated by drawing upon numerous resources concerning IoT design, primarily focusing on architectural principles. As illustrated in Fig. 6, the system design diagram framework is outlined. Within this research, a comprehensive examination of each component of the IoT architecture was conducted, culminating in recommendations for IoT system standards derived from a synthesis of literature reviews and technical analysis. The panel used in this research is an FACP panel with an addressable panel type with the Hochiki Latitude brand. The system created can only carry out monitoring, it is not equipped with control and automation functions

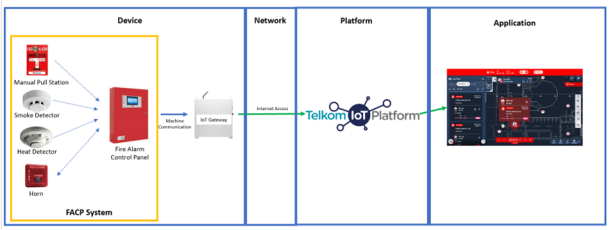

Fig. 6. System design.

B. IoT Device Testing

In the IoT Device section, several components are tested starting from the validation of FACP Sensor data sent to IoT Gateway. An illustration of sensor data validation can be seen in Fig. 7.

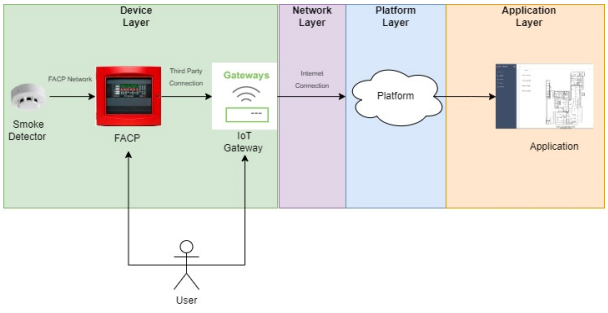

Fig. 7. IoT device validation.

Validation is performed by looking at the sensor status on the FACP panel and compared with the sensor status value on the IoT Gateway. Testing is carried out by carrying out an event trigger on the FACP panel so that it triggers the FACP panel to send information. The trigger events carried out such as triggering a fire on the heat detector, providing smoke on the smoke detector, removing the heat detector sensor and smoke detector, pulling the manual pull station, and creating an issue with the FACP panel grounding. The trigger event is carried out 100 times to get a good validation value.

In addition, validation is also carried out for power supply transitions from Primary to Secondary sources. Primary power is sourced from 220 V AC electricity, while secondary power utilizes VRLA batteries. The test involves disconnecting primary power to assess uninterrupted backup by the secondary source. Upon reconnection of primary power, the secondary source charges until fully replenished. The illustration of the power connection process can be seen in Fig 8.

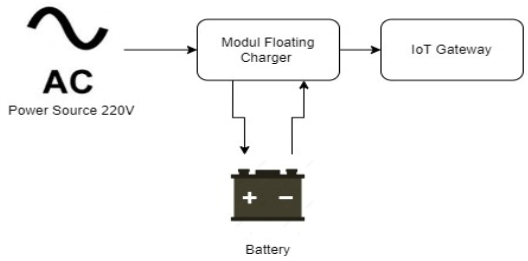

Fig. 8. Power connectivity block diagram on IoT gateway.

C. IoT Network Testing

The IoT network selection entails the utilization of a high-speed broadband internet connection, which is commonly employed as the connectivity medium for IoT devices. Similar to the provision of power, internet connectivity serves the Fire Alarm Control Panel (FACP) systems by employing at least two distinct connection sources. This redundancy ensures operational continuity in case one internet connection source experiences disruption. Furthermore, compliance with NFPA standards mandates the necessity of IP connectivity for FACP systems [14]. Broadband connections are used because FACP systems need to transmit information as quickly as possible to IoT platforms to determine near real-time conditions in the field. Some broadband communication comparison options can be seen in Fig. 9.

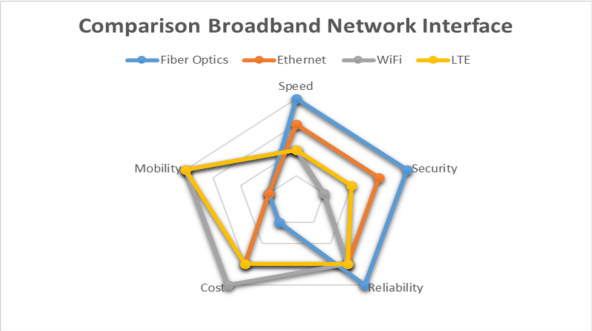

Fig. 9. Broadband network IoT comparison[17–20].

In general, the broadband physical network available in Indonesia is fiber optic, but at the final termination point, there is an Optical Network Termination (ONT) device that can function as a router as well [21]. In addition, LTE network connectivity can be accessed through the related provider tower using a modem device [22]. An illustration of available broadband networks can be seen in Fig. 10.

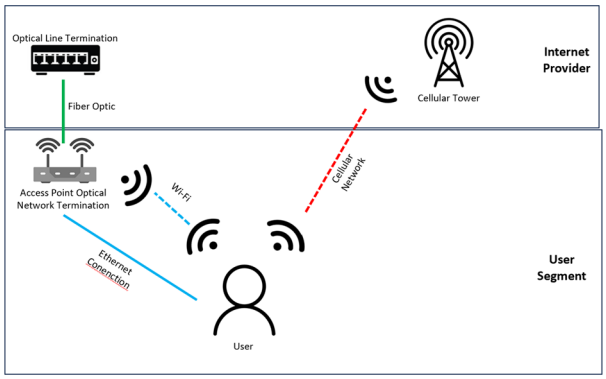

Fig. 10. Illustration of commonly available broadband Internet networks in Indonesia.

It can be known if the commonly used broadband internet network comes from fiber optics and cellular communications. However, at the termination point, customers can be accessed via Ethernet and WiFi for networks sourced from fiber optics, and use modems on cellular networks. Based on that, this study only tested connections using ethernet as the primary network, and connections using cellular networks as secondary networks.

In IoT Network testing, failover redundancy testing is carried out which is a test that aims to ensure the internet network connection on the IoT Gateway remains available even if one of the connections on the IoT network is lost. In this study, internet connections are divided into primary connections and secondary connections. The trial is carried out with conditions as in Table I.

TABLE I. TESTING FAILOVER REDUNDANCY

Primary Connection	Secondary Connection	Status Network
ON	ON	Primary Network
ON	OFF	Primary Network
OFF	ON	Secondary Network

D. IoT Platform QoS Testing

In the IoT Platform segment, it is imperative to scrutinize standards about the duration of data retention. Adhering to the NFPA 72 standard, the Fire Alarm Control Panel (FACP) mandates fire alarm systems to maintain logs of system status, encompassing alarms, issues, and surveillance signals, for a minimum duration of 60 hours [23]. However, some other jurisdictions require that FACPs retain data with longer retention periods, such as 90 days or more [4]. Apart from data storage, the section also necessitates the contemplation of data transmission protocols. Table II presents various options for data transmission protocols suitable for IoT applications.

TABLE II. IOT PROTOCOL COMPARISON [24–26]

IoT Data Protocols	Pro	Cons
Message Queue Telemetry Transport (MQTT)	Ensures message delivery, low overhead and bandwidth, uses TCP/IP as the underlying transport layer, and has a lot of support from within the IoT community.	Limited features and standardization, and depends on the network availability.
HyperText Transfer Protocol (HTTP)	Widely used and enables communication between web servers and clients.	Not specifically designed for IoT.
Constrained Application Protocol (CoAP)	UDP is for establishing secure communication between endpoints and is commonly used in IoT applications that require low power consumption and low bandwidth.	Limited features and standardization. And not designed for Real-time data transmission because Low Powered
Advanced Message Queue Protocol (AMQP)	They are commonly used in IoT applications that require reliable messaging and communication.	Heavy on bandwidth and only interfaces with web services via a gateway.

Based on NFPA, the standard delay of information and Alarm signals is 100 seconds [23]. Based on Table II, it is known that the CoAP protocol is not designed for communication in real-time and the AMQP protocol requires a large bandwidth so the IoT protocols that are most relevant to the FACP system are MQTT and HTTP protocols with the advantages of lightweight protocols and able to send data in real-time assuming a good connection from the network side and do not rule out the possibility of being able to use other protocols as long as they still follow signaling standards.

Communication performance testing on service quality is carried out to measure delay and packet loss following the ITU-T G.1010 standard using protocols MQTT and HTPP. Measurements are carried out by sending data 300 times for each measurement, measurements are carried out during working hours (09.00–17.00 WIB) and outside working hours for 1 week so that conditions are obtained on working days and at the end of the week

E. IoT Application Testing

In the IoT application section, in general, there is no specific standard regarding the display that must be used in the application. Still, if referring to the general display on the FACP panel screen, the application must have information in the form of:

- Current status of the fire alarm system, including fire location, alarm type, and detector and alarm status.
- A specific device that initiates a signal, such as a smoke detector or manual pull station[3, 10].

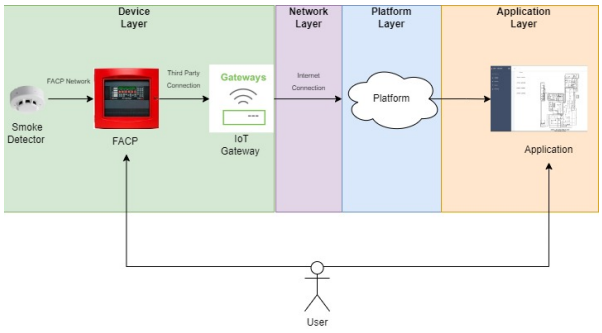

Fig. 11. Illustration of system test scenario.

IoT application testing is carried out by validating data methods according to those contained in the NFPA 72 standard, starting from Initiator testing, with several types of alarms. The test was conducted with all information possible from FACP data samples and validated on a designed IoT application. An illustration of the IoT System test can be seen in Fig. 11. Testing is carried out on 100 samples by providing samples of fire, and smoke and removing sensors, then validating the alarm values contained in the FACP panel with the IoT application designed.

Apart from that, in the application section, a Usability Test is carried out including Single Easy Question (SEQ) Testing, System Usability Scale (SUS), and Net Promoter Scorer (NPS). Testing was carried out by 5 users. Usability Testing is carried out in an integrated manner with the following task in Table III.

TABLE III. USABILITY TEST TASK

No	Task
1	Assess the ease of knowing the list and status of FACP sensor devices
2	Assess the ease of knowing the location of the FACP sensor device
3	Assess the ease of knowing information about the condition of IoT devices
4	Assess the ease of knowing Alarm information on FACP
5	Assess the ease of knowing the history of the FACP

IV. RESULT AND DISCUSSION

A. Design Result

The results of the system design for testing include the FACP Hochiki Latitude panel which has been integrated with several heat detectors, Smoke Detectors, Manual pull stations, and a strobe horn. The FACP system is integrated with the designed IoT Gateway panel. The results of the system design in this study can be seen in Fig. 12.

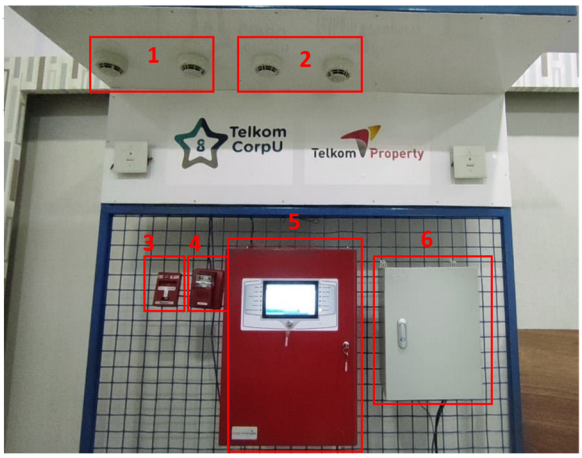

Fig. 12. Result of system design.

The initial display form of the web-based dashboard according to the design can be seen in Fig. 13

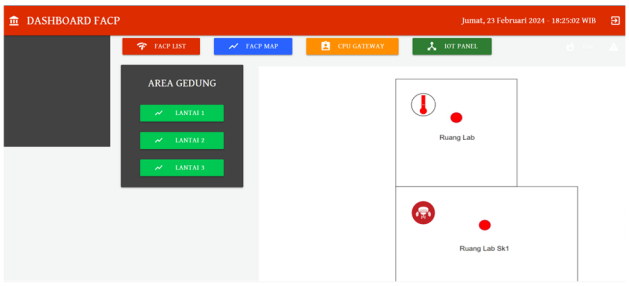

Fig. 13. Result of IoT application design.

B. IoT Device Testing Result

Information validation testing is carried out by performing trigger events 100 times on the FACP panel and validating on the IoT Gateway panel by viewing the information received from the FACP panel. The results of validation testing can be seen in Table IV.

Based on the test results, it can be concluded that IoT Gateway can receive all data properly without data corruption, data loss, or misinformation so recommendations for using machine communication to connect to IoT Gateways as media can be recommended to be a minimum standard.

TABLE IV. RESULTS OF FACP DATA VALIDATION ON IOT GATEWAY

No	Device	Event	Data on FACP	Data on IoT Gateway	Result
1	Power Supply Unit	Ground trouble	Trouble	Trouble	Appropriate
2	Manual Pull Station	Pull trigger	Fire	Fire	Appropriate
3	Heat Detector	Fire Trigger	Fire	Fire	Appropriate
…..	……..	……	……	……..	……..
100	Smoke Detector	Smoke Trigger	Fire	Fire	Appropriate

In testing the duration of capacity there are differences according to the calculation results. It is known that the battery capacity used is 7 AH with a voltage of 14 Volts. By calculating using (1) duration backup can be known as:

$$Battery\ Capaity = Current\ x\ Backup\ Time$$

$$Backup\ Time = \frac{Battery\ Capacity}{Current}$$

$$Backup\ Time = \frac{7\ Ah}{0{,}87\ A} = 8{,}02\ hours \quad (1)$$

However, based on the results of measuring the duration of the backup, the battery can only back up for 7,1 hours (7 hours 6 minutes), it is influenced by the use of the LVD module in the circuit as a module that cuts off the power supply in the system when it reaches a voltage of 12 V. The voltage is 12 V compared to the battery capacity of about 10%. So that the battery can only be used as much as 90%. Although battery usage cannot reach 100% on the system tested, the test results are still by the standards set by NFPA 72, which can back up at least 5–15 minutes.

Based on the test results, it can be recommended to become a standard related to the use of floating charge mode on the IoT Gateway panel power supply and the addition of capacity calculations with an additional minimum margin of 10% of the required current by the test results and NFPA 72 standard, with a minimum backup duration of IoT gateway during alarm mode on the FACP panel which is 5–15 minutes.

C. IoT Network Testing Result

Testing on an IoT network only performs over tests performed on the IoT Gateway module Network. Fail Over test is carried out to determine the transfer of primary network use to the secondary network without interruption (seamless). The test is carried out by pinging the IoT Gateway with the destination IP 8.8.8.8 along with the testing scenario in Table I. The test results can be seen in Table V.

TABLE V. FAIL OVER TEST RESULTS ON IOT NETWORK

No	Primary Connection	Secondary Connection	Status Network	Result
1	ON	ON	Primary Network	Appropriate
2	ON	OFF	Primary Network	Appropriate
3	OFF	ON	Secondary Network	Appropriate

D. IoT Platform QoS Testing Result

QoS testing was performed on delay and packet loss using MQTT and HTTP delivery protocols to IoT Applications and internet connection from Ethernet LAN and mobile internet. Delay measurement is done using node-red software and the results of delay measurement can be seen in the graph in Fig. 14 and Table VI.

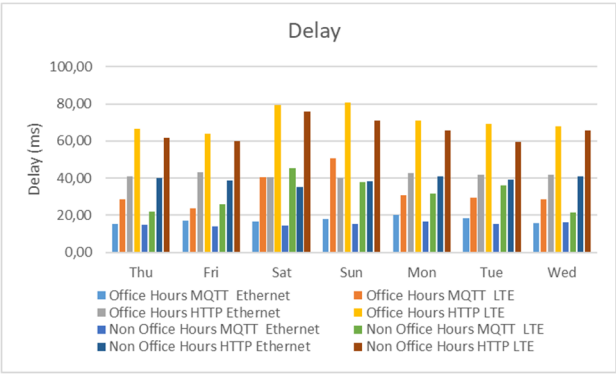

Fig. 14. QoS delay measurement results.

Based on the graph in Fig. 14 and Table V, it can be known several things such as:

- Average delay using MQTT Protocol is smaller than HTTP in each measurement
- Average delay using an Ethernet LAN connection is smaller than using Mobile LTE as an Internet connection
- Average delay in measurement outside working hours is smaller than delay in measurement in working hours
- The difference in the average delay on the work day and weekend is not very significant on every measurement

TABLE VI. QOS DELAY MEASUREMENT RESULT

Day	Delay (ms)							
	Office Hours				Non Office Hours			
	MQTT		HTTP		MQTT		HTTP	
	LAN	LTE	LAN	LTE	LAN	LTE	LAN	LTE
Thu	15.16	28.58	41.11	66.74	14.98	21.77	40.11	61.89
Fri	17.25	23.56	43.37	63.94	13.94	26.07	38.79	59.73
Sat	16.46	40.31	40.58	79.45	14.65	45.37	35.23	75.82
Sun	17.98	50.61	40.11	80.51	15.33	37.85	38.51	70.81
Mon	20.21	30.69	42.77	70.92	16.49	31.66	41.17	65.53
Tue	18.51	29.67	41.99	69.29	15.37	35.89	38.99	59.68
Wed	15.87	28.54	41.78	67.9	16.44	21.45	40.95	65.48
Average	17.35	33.14	41.67	71.25	15.31	31.44	39.11	65.56

Based on the measurement results. when compared with the ITU-T G.1010 Segment command/control data standard. the delay in every measurement result follows the maximum standard delay value of < 250 milliseconds.

Furthermore. the measurement of packet loss IoT Gateway data transmission on IoT Application using node-red software and based on the result. it is known that the packet loss value in each test with an ethernet LAN and mobile internet connection. in office hour and non-office hour. in the office day and weekend as well as with MQTT and HTTP protocols has a value of 0% in each measurement. Based on the measurement results. when compared with the ITU-T G.1010 standard command/control data segment. the packet loss in the measurement results follows the standard value of packet loss. which is 0%.

Based on the results of these tests. the proposal on the use of cable-based internet networks as primary connections. and mobile-based internet networks as secondary connections can be recommended to be standards for internet access connections. In addition. MQTT and HTTP protocols can also be recommended as protocols that can be used in IoT systems. This is indicated by QoS testing carried out following the ITU-T G.1010 standard even though the MQTT protocol is more recommended than HTTP because the MQTT protocol has a smaller delay value and is intended for machine-to-machine communication compared to HTTP.

E. IoT Application Testing Result

Application validation testing is carried out by performing trigger events 100 times on the FACP panel and validating the IoT Application by viewing the information received from the FACP panel. Validated parameters include sensor ID information. events. and event timestamps. The results of validation testing can be seen in Table VII.

TABLE VII. IOT APPLICATION TESTING RESULT

No	Device Id	Device	Event	Validasi
1	001	Heat Detector	Fire Trigger	Appropriate
2	001	Heat Detector	Fire Cleared	Appropriate
3	001	Heat Detector	Trouble Device	Appropriate
4	001	Heat Detector	Trouble Cleared	Appropriate
5	002	Smoke Detector	Fire Trigger	Appropriate
…	…..	…….	…...	…...
99	003	Smoke Detector	Fire Trigger	Appropriate
100	003	Smoke Detector	Fire Cleared	Appropriate

Based on the test results. it can be concluded that IoT Applications can receive all data properly with 100% data validation.

TABLE VIII. SINGLE EASY QUESTION RESULT

Responded No	Jobs	Task 1	Task 2	Task 3	Task 4	Task 5
1	IoT Engineer	6	7	6	6	5
2	IoT Engineer	6	6	7	7	6
3	NOC Support	6	5	6	6	6
4	Project Manager	5	6	6	5	5
5	Building Manager	7	6	5	5	5
Average		6.0	6.0	6.0	5.8	5.4

Next. the results of carrying out the Single Easy Question (SEQ) table regarding the level of ease of accessing tasks can be seen in Table VIII.

Based on Table VIII. it is known that the results of the application design were made based on several pieces of information. It can be concluded that the average ease value for each task reached a value of 5.4–6. which means the application is easy to use according to the function of the research objectives. Next the System Usability Scale testing. the results of the System Usability Scale test can be seen in Table IX.

TABLE IX. SYSTEM USABILITY SCALE RESULT

Reponden	Score										Rate
	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	
Responden 1	4	1	5	1	5	2	5	1	5	1	95
Responden 2	4	2	5	2	5	3	5	3	5	2	80
Responden 3	4	2	4	2	4	2	4	2	4	2	75
Responden 4	4	2	5	2	5	2	5	3	5	2	83
Responden 5	4	2	4	2	4	2	4	2	4	2	75
Average											82

Based on Table IX it can be concluded that the average results of the system usability scale carried out by 5 respondents get a value of 82 which means that this application reaches the EXCELENT grade.

Next. the Net Promotor Scorer. the results of the Next Propotor Scorer regarding the Net Promoter Scorer. the following results were obtained:

- Promoter: 5 (100%)
- Passive: 0 (0%)
- Detractors: 0 (0%)
- NPS = Promoters–Detractors = 100%−0% = 100%

V. CONCLUSION

Based on the results of the research conducted. several recommendations can be drawn regarding IoT standards for FACP. Firstly. IoT gateways should be connected via third-party interfaces from FACP. validated at 100%. Secondly. these gateways must utilize two power sources. direct power supply. and battery backup with a floating charge circuit. ensuring compliance with NFPA 72 standards with a backup duration of 5 to 15 minutes. and increasing battery capacity by at least 10%. Thirdly. IoT gateways should incorporate dual internet connectivity and network devices with seamless features to ensure network backup. Fourthly. cable-based networks should be prioritized over wireless networks. as indicated by QoS measurements favoring Ethernet connections. Additionally. the MQTT protocol is recommended over HTTP for data transmission due to better QoS. with MQTT exhibiting the smallest average delay value of 15.51 ms during off-peak hours. Finally. IoT applications for FACP should provide comprehensive information on the fire alarm system's status. including fire location. alarm type. detector. and alarm status. and the specific device that triggered the signal. validated through usability tests with high satisfaction scores and validation rates. IoT applications for FACP should offer real-time updates on fire alarm systems. validated with a 100% usability test score. SEQ 5.4-6. SUS 82. and NPS 100%. These quantifiable metrics underscore the efficacy of the proposed IoT standards for FACP. ensuring robust connectivity. power efficiency. and operational effectiveness.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

In this research project, Fikri Nizar Gustiyana acts as Engineer of Research with a focus on technical tasks such as experimental design and data analysis. Rendy Munadi, Nyoman Karna, and I Ketut Agung Enriko, act as Research Supervisors who supervise and direct the overall progress of the research, providing guidance to Fikri Nizar Gustiyana and his team, while I Ketut Agung Enriko also acts as Sponsor with responsibility for providing financial resources and ensure project alignment with organizational goals. All authors had approved the final version.

ACKNOWLEDGMENT

The authors wish to thank Telkom Corporate University as a funder and support for this research.

REFERENCES

[1] A. Rashid. (2023). *Fire Alarm Control Panel (FACP) | Types and How Does It Work?* [Online]. Available: https://www.hseblog.com/fire-alarm-control-panel-facp/

[2] D. Security. (2020). *What Is a Fire Alarm Control Panel (FACP)?* [Online]. Available: https://blog.dga.com/what-is-a-fire-alarm-control-panel-facp

[3] S. Mahoney. (2021). A Guide to Fire Alarm Basics – Initiation | NFPA. [Online]. Available: https://www.nfpa.org/News-and-Research/Publications-and-media/Blogs-Landing-Page/NFPA-Today/Blog-Posts/2021/04/14/A-Guide-to-Fire-Alarm-Basics-Initiation?icid=W483

[4] N. Young, "Fire detection and alarm systems," *Fire Prev. Fire Eng. Journals*. vol. 64, no. 243, pp. 53–55, 2004. doi: 10.1049/wis.1977.0001

[5] Safaruddin, "Standarisasi," *J. Kotamo*. vol. 2, no. 3, pp. 1–9, 2022.

[6] W. Pradono and Y. Yourdan, "Policy analysis on telecommunication devices security standardization to support national security and defence policy," *Bul. Pos dan Telekomun.*, vol. 13, no. 2, 2015. doi: 10.17933/bpostel.2015.130204

[7] P. E. Prasetyo. (2015). Standarisasi Dan Komersialisasi Produk Industri Kreatif Dalam Mendukung Pertumbuhan Ekonomi Daerah. [Online]. Available:

https://www.unisbank.ac.id/ojs/index.php/sendi_u/article/view/5092
[8] T. Instrument. (2023). *Fire Alarm Control Panel (FACP)*. [Online]. Available: https://www.ti.com/solution/fire-alarm-control-panel-facp
[9] H. Annex, *National Fire Alarm and Signaling Code 2013 Edition*, pp. 16–362, 2013.
[10] F. I. Association. (2023). EN-54 Document. [Online]. Available: https://www.fia.uk.com/resources/british-standards/bs-en-54-series-fire-detection-alarm-systems.html
[11] Strom (2023). How networked systems enable instant access to critical life safety data. [Online]. Available: https://www.hochikieurope.com/blog/emergency-lighting-how-networked-systems-are-enabling-instant-access-to-critical-life-safety-data
[12] I. M. A. Shereiqi and M. M. Sohail. "Smart fire alarm system using IOT," *J. Student Res.*. pp. 1–9. 2020. doi: 10.47611/jsr.vi.882
[13] I. K. A. Enriko, A. N. Nababan, A. F. Rochim, and S. Kuntadi, "A fire suppression monitoring system for smart building," *J. Infotel*. vol. 15, no. 2, pp. 74–79, 2023. doi: 10.20895/infotel.v15i2.940
[14] G. Kessinger. (2023). NFPA 72 permits internet monitoring. [Online]. Available: https://www.securityinfowatch.com/alarms-monitoring/fire-life-safety/article/10542097/nfpa-72-permits-internet-monitoring
[15] L. Puspitawati, A. Nurhasanah, and A. S. Khaerunnisa, "Utilization of communication technology for business," *Int. J. Informatics. Inf. Syst. Comput. Eng.*. vol. 2, no. 1, pp. 47–54, 2021. doi: 10.34010/injiiscom.v2i1.4864
[16] D. Khanna and A. Sharma, "Internet of things challenges and opportunities," *Int. J. Technol. Res. Eng.*. vol. 6, no. 12, 2019. doi: 10.1007/978-981-16-9260-4_2
[17] A. K. Group. (2023). Fiber internet vs 4G/5G- What's the difference and Which is better? [Online]. Available: https://www.zajil.com/fiber-internet-vs-4g-5g/
[18] D. Ngo. (2023). Tips on getting high-speed internet: It's fiber vs cable (coaxial) or ONT vs modem. [Online]. Available: https://dongknows.com/fiber-vs-cable-internet-docsis-modem-vs-ont/
[19] K. Pahlavan and P. Krishnamurthy, "Evolution and impact of Wi-Fi technology and applications: A historical perspective," *Int. J. Wirel. Inf. Networks*. vol. 28, no. 1, pp. 3–19, 2021. doi: 10.1007/s10776-020-00501-8
[20] V. A. Orfanos, S. D. Kaminaris, P. Papageorgas, D. Piromalis, and D. Kandris, "A comprehensive review of IoT networking technologies for smart home automation applications," *J. Sens. Actuator Networks*, vol. 12, no. 2, 2023. doi: 10.3390/jsan12020030
[21] W. T. Mukti and E. Safrianti. "Fiber To The Home (FTTH) network design STO arengka link to villa melati permai II widyantoro housing complex," *Jom FTEKNIK VOL.*, vol. 4, no. 2, pp. 1–14, 2017, (In Indonesian).
[22] A. Wulandari, T. Supriyanto, and M. Itsnan, "Design and analysis of LTE home implementation on the 4G LTE network on the 2300 Mhz frequency," *JST (Jurnal Sains Ter.*. vol. 5, no. 1, 2019 (in Indonesian). doi: 10.32487/jst.v5i1.585
[23] NFPA, "NFPA 72 chapter 9," *NFPA 72*, vol. 66, 2017, pp. 37–39.
[24] T. Melodia, D. Pompili, and I. F. Akyildiz, "On the interdependence of distributed topology control and geographical routing in ad hoc and sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 3, pp. 520–531, 2005. doi: 10.1109/JSAC.2004.842557
[25] A. Bhardwaj, K. Kaushik, S. Bharany, M. F. Elnaggar, M. I. Mossad, and S. Kamel, "Comparison of IoT communication protocols using anomaly detection with security assessments of smart devices," *Processes*, vol. 10, no. 10, 2022. doi: 10.3390/pr10101952
[26] V. Sarafov and J. Seeger. "Comparison of IoT data protocol overhead," *Semin. Futur. Internet SS2017. Dep. Informatics. Tech. Univ. Munich.*, pp. 7–14. 2018. doi: 10.2313/NET-2018-03-1